

National Infrastructure Advisory Council (NIAC)

Convergence Working Group

Status Report
April 11, 2006

George H. Conrades
Executive Chairman
Akamai Technologies

Greg Peters
Former Chairman and CEO
Internap Network Services

Margaret Grayson
President, AEP Govt.
Solutions Group

Overview

- ▣ Purpose
- ▣ Status of *Next Steps* from Last Meeting
- ▣ Timeline
- ▣ Actions
- ▣ Key Observations to Date
- ▣ Next Steps

Purpose

- Mission: The Convergence Study Group will investigate important questions and make recommendations regarding the protection of SCADA and Process Control Systems from cyber threats.

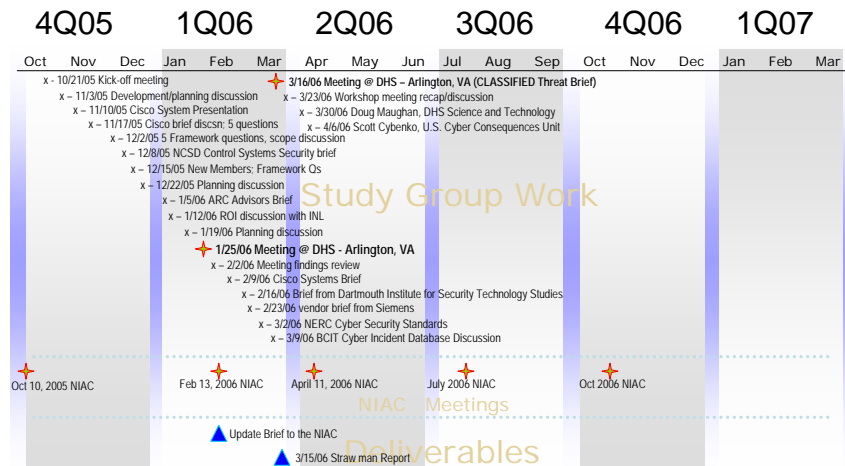
3

Status of *Next Steps* from Last Meeting

- ✓ Continue group development with key input from Industry and Government
 - Classified Threat Brief
 - Andrew Wright and Venkat Pothamsetty, Cisco Systems CAIG
 - Professors Cybenko and Smith, Dartmouth Cyber Security Program
 - Paul Skare, Siemens
 - Tom Flowers, NERC
 - Professors Eric Byres and David Leversage, BCIT
 - Doug Maughan, DHS Science and Technology
- ✓ Draft report submitted to Working Group Chair point of contact for review.
 - Includes full synopsis of all findings on the five framework questions
 - Established interrelationships between five framework questions

4

Time Line



5

Actions

- ❑ Held second workshop meeting
- ❑ Received secret-level threat brief to help develop understanding of existing threat to SCADA and Process Control Systems
- ❑ Identified key elements, interrelationships and next steps for developing policy-level recommendations for the five framework questions.
- ❑ Developed four draft recommendations
- ❑ Continuing to work with subject matter experts on key elements

6

Key Observations to Date

- ❑ There is significant diversity both within and across sectors in terms of response to this emerging threat.
- ❑ The motivating factor for businesses that have addressed SCADA/PCS security is *consequence*.
 - threats from cyber security were directly correlated to failures in reliability, availability and safety
- ❑ Opportunities exist for the federal government to lead in information sharing, research and development coordination, creating market stimuli, and facilitating executive leadership access to important information.

7

Key Observations to Date (*continued*)

- ❑ Standards and application of existing standards are inconsistent across sectors
- ❑ Access to threat and consequence information is critical to motivating executive leadership to act on the emerging cyber threat.
- ❑ Threat and consequence information are missing elements in the return on investment equation for cyber security case that must be made to executives.
- ❑ There is no universally accessible mechanism for sharing threat and incident information, and barriers exist for companies to do so.

8

Next Steps

- ▣ Address consequences element with Scott Borg, U.S. Cyber Consequences Unit and Insurance industry
- ▣ Conduct CEO outreach
- ▣ Further develop potential recommendations
- ▣ Consult University of Georgia Department of Risk Management

9

Discussion

- ▣ Questions?

10